

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229859
 (43)Date of publication of application : 16.08.2002

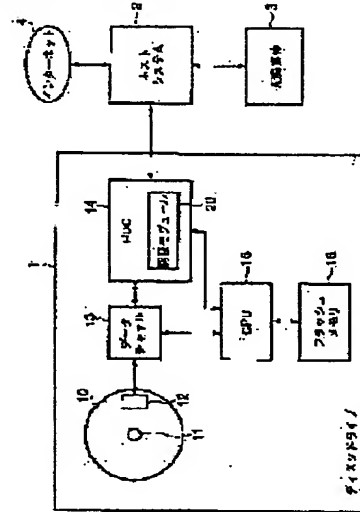
(51)Int.Cl. G06F 12/14
 H04L 9/14
 H04L 9/32

(21)Application number : 2001-023362 (71)Applicant : TOSHIBA CORP
 (22)Date of filing : 31.01.2001 (72)Inventor : IGARI CHIKASHI

(54) DISK MEMORY AND AUTHENTICATING METHOD APPLIED THERETO

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a disk memory establishing a plurality of secret ranges and having a different authenticating function for each secret range.
SOLUTION: A disk 10 wherein a plurality of secret ranges is established is provided. An authentication module 20 allows only a host system 2 authenticated by the authenticating function to access to each secret range. By exchanging information with the host system 2, the authentication module 20 uses key information established for each secret range and range inherent information to conduct a certifying procedure for deciding whether access is permitted or not for each secret range.



LEGAL STATUS

[Date of request for examination] 13.12.2004
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

REST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-229859
(P2002-229859A)

(43) 公開日 平成14年8月16日 (2002.8.16)

(51) Int.Cl. ⁷	識別記号	F I	チーエムコード (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 5 B 0 1 7
			3 2 0 B 5 J 1 0 4
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1
9/32			6 7 5 A

審査請求 未請求 請求項の数 9 O L (全 9 頁)

(21) 出願番号 特願2001-23362 (P2001-23362)

(22) 出願日 平成13年1月31日 (2001.1.31)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 猪狩 史

東京都青葉市本広町2丁目9番地 株式会

社東芝青葉工場内

(74) 代理人 100058479

弁理士 鈴木 武彦 (外6名)

Fターム (参考) 5B017 AA06 BA07 BA09 CA05 CA07

5J104 AA07 AA13 KA02 KA04 NA02

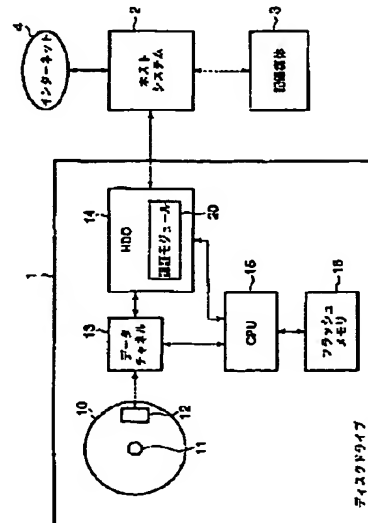
NA27 NA35 PA07

(54) 【発明の名称】 ディスク記憶装置及び同装置に適用する認証方法

(57) 【要約】

【課題】 ディスク上に複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能を有するディスク記憶装置を提供することにある。

【解決手段】 複数の秘匿領域が設定されたディスク10が設けられている。各秘匿領域は、認証モジュール20により認証機能で認証されたホストシステム2のみによりアクセスが可能となる。認証モジュール20はホストシステム2との情報交換により、各秘匿領域ごとに設定されている鍵情報と領域固有情報を使用して、各秘匿領域毎にアクセスを許可するか否かを決定するための認証手順を実行する。



- 1 -

(2) 特開2002-229859

2

【特許請求の範囲】

【請求項1】 複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、

前記各秘匿領域に対応する複数の鍵情報及び当該各秘匿領域に共通な固有情報を記憶している記憶手段と、
前記鍵情報と前記固有情報とから生成される前記各秘匿領域毎の領域固有情報を使用して、当該各秘匿領域毎にアクセスを許可するか否かを決定するための認証処理を実行する認証手段とを具備したことを特徴とするディスク記憶装置。

【請求項2】 前記認証手段は、

乱数とアクセス対象の秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行する暗号化手段と、

当該秘匿領域のアクセスを要求する外部装置に対して前記鍵情報及び前記固有情報を送出する手段と、

前記外部装置から前記乱数及び前記領域固有情報に相当する各情報を使用した暗号化演算結果を受信し、当該暗号化演算結果と前記暗号化手段による暗号化演算結果とが一致した場合に、アクセス対象の秘匿領域に対するアクセスを許可する判定手段とを有することを特徴とする請求項1記載のディスク記憶装置。

【請求項3】 前記認証手段は、

乱数又は疑似乱数を生成する乱数生成手段を有し、
当該乱数生成手段により生成した乱数を前記暗号化手段に与えると共に、前記外部装置に送出する手段とを有することを特徴とする請求項2記載のディスク記憶装置。

【請求項4】 前記認証手段は、

指定の秘匿領域のアクセスを要求する外部装置に対して当該秘匿領域に対応する鍵情報及び前記固有情報を送出する手段と、

前記外部装置から供給された乱数と、アクセス対象の秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行する暗号化手段と、

前記外部装置から、前記鍵情報及び前記固有情報を使用して得られた前記領域固有情報に相当する情報と前記乱数とを使用した暗号化演算結果を受信する手段と、

前記外部装置からの暗号化演算結果と前記暗号化手段による暗号化演算結果とが一致した場合に、アクセス対象の秘匿領域に対するアクセスを許可する判定手段とを有することを特徴とする請求項1記載のディスク記憶装置。

【請求項5】 前記認証手段は、

乱数とアクセス対象の秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行する暗号化手段と、

当該秘匿領域のアクセスを要求する外部装置に対して前記鍵情報及び前記固有情報を送出する手段とを有し、

前記外部装置において前記乱数及び前記領域固有情報に

相当する各情報を使用した暗号化演算結果と、前記暗号化手段による暗号化演算結果とを比較する認証処理で両者の演算結果が一致した場合に、各秘匿領域毎にアクセスを許可するか否かを決定するための前記認証処理を実行するように構成されていることを特徴とする請求項1記載のディスク記憶装置。

【請求項6】 前記各秘匿領域毎の領域固有情報を記憶する手段と、

外部装置からの更新要求に応じて前記鍵情報と前記領域固有情報を更新する更新手段とを特徴とする請求項1から請求項5のいずれか記載のディスク記憶装置。

【請求項7】 複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、前記各秘匿領域に対応する複数の鍵情報及び当該各秘匿領域に共通な固有情報を記憶している記憶手段とを有するディスク記憶装置に適用する認証方法であって、

ホストシステムによりアクセス対象として指定される秘匿領域毎に、前記記憶手段から当該秘匿領域に対応する前記鍵情報及び前記固有情報を読出すステップと、
前記鍵情報及び前記固有情報を使用して当該秘匿領域に対応する領域固有情報を生成するステップと、
前記領域固有情報を使用して、当該秘匿領域のアクセスを許可するか否かを決定するステップと、から構成されることを特徴とする認証方法。

【請求項8】 前記ホストシステムに対して前記鍵情報及び前記固有情報を送出するステップと、

乱数と当該秘匿領域に対応する領域固有情報とを使用して所定の暗号化演算処理を実行するステップと、

前記ホストシステムから前記乱数及び前記領域固有情報に相当する各情報を使用した暗号化演算結果を受信するステップと、

前記ホストシステムからの暗号化演算結果と、前記暗号化演算処理ステップにより算出された暗号化演算結果とが一致した場合に、アクセス対象の秘匿領域に対するアクセスを許可するステップとを有することを特徴とする請求項7記載のディスク記憶装置。

【請求項9】 複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、前記各秘匿領域に対応する複数の鍵情報、当該各秘匿領域毎の領域固有情報、及び乱数種の暗号化・復号化機能に関する機能情報を記憶している記憶手段とを有するディスク記憶装置に適用する認証方法であって、

ホストシステムにより指定された機能情報を前記記憶手段から読出して、当該ホストシステムに送出するステップと、

前記送出ステップにより送出した機能情報に基づいて、前記ホストシステムにより構成された鍵情報を前記ホストシステムから受信するステップと、

3

前記受信ステップにより受信した鍵情報を使用して、前記ホストシステムにより指定された秘匿領域に対応する領域固有情報を生成するステップと、前記受信ステップにより受信した鍵情報及び前記生成ステップにより生成した領域固有情報を使用して、前記ホストシステムにより指定された秘匿領域に対する鍵情報及び領域固有情報を更新するステップと、から構成されることを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばハードディスクドライブに適用し、特にディスク上の秘匿領域に対するアクセスを制限するための認証機能を備えたディスク記憶装置に関する。

【0002】

【従来の技術】近年、インターネットやデジタル放送網などから、画像（動画及び静止画）や音声などのコンテンツデータ、またはプログラムを配信する情報サービスのシステムが注目されている。このようなシステムでは、配信されるデータは、パーソナルコンピュータなどを含むデジタル機器などにダウンロードされて、当該機器に装着されている記録媒体に保存される。デジタル機器には、デジタルテレビジョン装置や、携帯電話または専用再生機器などのモバイル情報機器が含まれる。

【0003】これらの機器に装着されている記録媒体は、フラッシュEEPROMなどからなるメモリカードや、ハードディスクドライブ（HDD）又は光磁気ディスクドライブ（MO）などのディスクドライブからなる。

【0004】ところで、情報サービスシステムでは、コンテンツデータやプログラムの著作権保護のために、特にコピー防止を目的とするセキュリティ機能が不可欠な要素になっている。このセキュリティ機能には、記録媒体の一部の記憶領域を秘匿領域として設定し、当該秘匿領域のアクセス時に認証処理を実行する認証機能が含まれる。認証機能は、当該秘匿領域に対するアクセス要求がある場合に、アクセスを許可するか否かを判定する認証手順からなる。

【0005】

【発明が解決しようとする課題】従来では、例えばフラッシュEEPROMからなるメモリカードを使用するシステムに対しては、各種の認証機能が開発されている。これに対して、HDDを代表とするディスクドライブを使用するシステムでは、ホストシステム（デジタル機器の本体）側の認証機能としては各種の方式があるが、ドライブ自体には制限された認証機能しか設けられていない。

【0006】ディスクドライブの認証機能としては、ディスク上の所定の記憶領域を秘匿領域として設定し、当

(3)

特開2002-229859

4

該秘匿領域に対するアクセスを制限するための認証手順が提案されている。秘匿領域には、例えば暗号化／復号化処理に必要な鍵情報が格納される。この鍵情報を使用して、非秘匿領域（通常記憶領域）に格納されたコンテンツデータの暗号化又は復号化を行なう機能が実現される。

【0007】従来の認証機能は、1種類の認証手順により秘匿領域に対するアクセスの許可を判定する方式が一般的である。メモリカードなどでは、記憶容量が制限されているため、秘匿領域も制限される。従って、通常では1種類の認証手順による認証機能が設定されている。しかしながら、ディスクドライブでは、相対的に大容量であるため、ディスク上に複数の秘匿領域を設定することが可能である。この場合、各秘匿領域毎に異なる認証機能を設定することが可能であれば、応用範囲の広いシステムを実現することが可能となる。

【0008】そこで、本発明の目的は、ディスク上に複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能を設定できるディスク記憶装置を提供することにある。

【0009】

【課題を解決するための手段】本発明は、記録媒体であるディスク上に、アクセスが制限されている複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能により認証処理を実行するディスクドライブに関する。

【0010】即ち、本ディスクドライブは、複数の所定記憶領域を特別のアクセス条件を必要とする複数の秘匿領域として設定可能なディスク記憶媒体と、各秘匿領域に対応する複数の鍵情報及び当該各秘匿領域に共通な固有情報を記憶している記憶手段と、鍵情報と固有情報とから生成される各秘匿領域毎の領域固有情報を使用して、当該各秘匿領域毎にアクセスを許可するか否かを決定するための認証処理を実行する認証手段とを有する。

【0011】具体的には、ディスクドライブは、暗号化・復号化機能を実行する暗号化回路を例えばディスクコントローラの内部に備えている。また、ディスクドライブは、ドライブ自体を識別するためのドライブの固有情報（ID情報）を、例えばドライブ内のフラッシュEEPROMに記憶している。各秘匿領域毎に設定された各鍵情報は、例えばディスク上の秘匿領域又はフラッシュEEPROMに記憶されている。

【0012】複数の秘匿領域には、例えば非秘匿領域に格納されて、暗号化されたコンテンツデータ（例えば暗号化された音楽データ）をアクセスするための（復号化）鍵情報が保存される。この場合、各秘匿領域ごとに、異なる暗号化・復号化方式に対応する鍵情報や、またはコンテンツの種類毎に異なる鍵情報を保存することが可能である。従って、本発明のディスクドライブを使用したシステムであれば、暗号化・復号化方式の異なるコンテンツデータを保存した場合に、当該各コンテンツデータを復号化するための各鍵情報を、秘匿領域のい

5

れから得ることが可能である。本発明では、各秘匿領域に対するアクセスを実行する場合に、各秘匿領域毎に異なる認証手順での認証処理が実行される。従って、複数種の暗号化・復号化方式を適用した情報に対する情報保護機能を実現したシステムを提供することが可能となる。

【0013】本発明の具体的適用分野としては、例えばパーソナルコンピュータやモバイル情報機器の交換型記憶装置として使用するためのカード型（又はモバイル型）ディスクドライブや、インターネットやLANなどに使用されるサーバ用ストレージ装置である。

【0014】本発明の別の観点としては、各秘匿領域に対応する鍵情報及び領域固有情報を更新する更新機能を有するディスクドライブである。この更新機能は、ホストシステムにより指定された秘匿領域に対応する鍵情報を、ディスクドライブが予め保存している暗号化・復号化機能情報に基づいてホストシステムにより構成された鍵情報に更新する機能である。ディスクドライブは、予め複数種の方式の暗号化・復号化プログラムを記憶している。暗号化・復号化機能情報は、当該暗号化・復号化プログラムのプログラム名または暗号化・復号化の方式名を示す情報である。

【0015】ディスクドライブは、該当する鍵情報を更新すると、当該鍵情報から領域固有情報を算出して、ホストシステムにより指定された秘匿領域に対応する領域固有情報を更新する。従って、暗号化・復号化方式の変更に伴って、該当する秘匿領域（暗号化・復号化処理に必要な鍵情報を保存する）に対して、認証手順を変更することが可能となる。

【0016】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【0017】（ディスクドライブの構成）同実施形態では、HDDであるディスクドライブ1と、ホストシステム2とを有するデジタル機器を想定し、ディスクドライブ1はホストシステム2からのコマンドに応じて各種の動作を実行する。

【0018】ホストシステム2は、マイクロプロセッサと各種アプリケーション・ソフトウェアとをメイン要素とし、インターネット4やデジタル放送ネットワークに接続している。ホストシステム2は、当該ネットワーク（インターネット4を含む）から配信されたコンテンツデータ（例えば音楽データや画像データなど）やプログラムを、ディスクドライブ1にダウンロードする機能を有する。さらに、ホストシステム2は、ダウンロードされた配信データ（暗号化データ）の復号化機能やコピー防止機能などのセキュリティ機能を備えている。また、ホストシステム2は、ディスクドライブ1から読出したコンテンツデータまたはインターネット4から配信されたコンテンツデータを、例えばメモ리카ードなどの記憶

(4)

特開 2002-229859

6

媒体 3 にコピーする機能を有する。この記録媒体 3 は、例えば携帯型再生機器（モバイル情報機器）の交換型記録媒体として使用される。

【0019】ディスクドライブ1は、記録媒体としてのディスク10と、データの記録又は再生を行なうヘッド12と、データチャネル13と、ディスクコントローラ(HDC)14と、CPU15と、フラッシュEEPROM(フラッシュメモリ)16とを有する。また、フラッシュメモリ16以外に、RAM及びROMなどのメモリも設けられている。

【0020】ディスク10は、データ記録再生時には、CPU15の制御によりスピンドルモータ11により高速回転している。ヘッド12は、CPU15の制御に基づいて、図示しないヘッドアクチュエータによりディスク10の半径方向に移動可能に構成されている。データチャネル13は、ヘッド12からのリード信号を再生データに変換し、ディスクコントローラ14からの記録データを記録信号に変換するための信号処理を行なうリード/ライト回路である。

20 【0021】HDC14は、ディスクドライブ1とホストシステム2とのインターフェース（例えばATAインターフェース仕様）を構成し、ホストシステム2からの各種のコマンド及びデータの転送を制御する。HDC14は、同実施形態の認証機能に関する認証モジュール20を有する。認証モジュール20は、専用LSIからなるハードウェアである。具体的には、認証モジュール20は、図6に示すように、暗号化・復号化回路200、乱数発生回路201、及び暗号化・復号化処理に必要な鍵データなどを格納するフラッシュEEPROM202等を備えている。暗号化・復号化回路200は、換述するようには、複数種の方式（A～C）の暗号化・復号化機能部を有する。また、暗号化・復号化回路200は、複数種の方式（A～C）の暗号化・復号化プログラムを記憶し、CPU15に当該プログラムを供給する構成でもよい。この場合には、CPU15は、暗号化・復号化プログラムを実行して、同実施形態に関する認証処理や、暗号化・復号化処理を実施する。

【0022】CPU15は、ドライブ1のメイン制御要素であり、データ読取再生動作及びヘッド位置決め制御などの他に、同実施形態に関する認証機能に関する制御動作を実行する。フラッシュメモリ16は、図3に示すように、超磁機能に必要なドライブ1の固有情報（ドライブID情報）160を格納するための不揮発性メモリである。また、フラッシュメモリ16は、認証処理や暗号化・復号化処理に必要な鍵情報などを格納するメモリとして使用されてよい。

【0023】（ディスクの構成）実施形態では、図2に示すように、ディスク10上の所定記憶領域（例えば内周側エリア）は、複数の記憶領域101~103（ここでは3領域とする）が決定される。各記憶領域101

7

～103は、例えばホストシステム2からの設定コマンドにより設定される特別の領域であり、アクセスが制限されている。ここで、ディスク10上の全記憶領域から秘密領域101～103を除いた非秘密領域100は、認証機能とは無関係な通常使用領域である。この通常使用領域100には、コピー制限されているコンテンツデータ（配信データ）などが暗号化されて格納（ダウンロード）される。

【0024】各秘密領域101～103は、例えばインターネット4から非秘密領域100にダウンロードされた暗号化データ（コンテンツデータ）を復号化したり、または当該コンテンツデータを暗号化するために必要な鍵情報などを格納する。さらに、各秘密領域101～103は、それぞれの領域のアクセスでの認証処理に必要な鍵情報101A～103Aを格納するためのエリア、及び後述する各領域固有情報101B～103Bを格納するためのエリアを有する。同実施形態の認証機能は、当該鍵情報101A～103A、各領域固有情報101B～103B及びフラッシュメモリ16に格納されたドライブID情報160を使用する。

【0025】（認証処理）以下主として図4及び図5のフローチャートを参照して、秘密領域101～103のアクセスに対する認証手順を説明する。なお、図4及び図5のフローチャートでは、ディスクドライブ1の処理と、ホストシステム2の処理とが併記されており、点線は情報やコマンドの交換を意味している。

【0026】ここでは、ホストシステム2が、ディスク10の非秘密領域100から暗号化データ（例えば音楽データなどのコンテンツデータ）を復号化して、メモリカードなどの記録媒体3にコピーする場合を想定する。このため、ホストシステム2は、所定の秘密領域（101とする）から当該コンテンツデータを復号化するための鍵情報を取得するため、ディスクドライブ1に対してアクセス要求を実行する。ディスクドライブ1は、当該アクセス要求に対して所定の認証処理を実行する。

【0027】まず、ホストシステム2からドライブ1を識別するためのドライブID情報160の読出し要求がなされると、ドライブ1はフラッシュメモリ16に格納された当該ドライブID情報160をホストシステム2に送出する（ステップH1、D1）。なお、ディスクドライブ1では、ホストシステム2とのデータや情報の転送は、HDC14及びCPU15により実行される。

【0028】次に、ホストシステム2は、アクセスすべき秘密領域101を選択し、当該秘密領域101に対する鍵情報101Aの読出し要求を行なう（ステップH2、H3）。この要求に応じて、ドライブ1は、ディスク10上の指定された秘密領域101から鍵情報101Aを読出して、ホストシステム2に送出する（ステップD2）。

【0029】ホストシステム2は、読出したドライブID

(5)

特開2002-229859

8

D情報160と鍵情報101Aとを所定の復号化機能部（暗号化・復号化プログラム）に与えて、当該秘密領域101に対応する領域固有情報（101Bに相当する情報）を算出（復号化）する（ステップH4）。即ち、同実施形態の認証機能は、秘密領域101に対応する領域固有情報101Bをドライブ1がホストシステム1に送出することなく、両者において共通の領域固有情報101Bを有する構成である。従って、秘密領域101にアクセスするための認証手順に必要な領域固有情報101Bが、外部に漏洩することは無く、高いセキュリティ性を備えた認証機能である。

【0030】さらに、ホストシステム2は、乱数発生機能部（乱数発生プログラム）から乱数（疑似乱数）を生成し、予め備えている暗号化機能部（暗号化プログラム）に当該乱数と、算出した領域固有情報とを与えて、暗号化情報（暗号化演算結果）を算出する（ステップH5、H6）。ホストシステム2は、生成した乱数をディスクドライブ1に送出する（ステップH7）。一方、ディスクドライブ1では、認証モジュール20は、暗号化・復号化回路200での所定の暗号化手順（例えばプログラムA）により、当該乱数と領域固有情報101Bとを使用して、暗号化演算を実行し、演算結果である暗号化情報を算出する（ステップD3）。ドライブ1は、算出した当該暗号化情報をホストシステム2に送出する（ステップD4）。

【0031】ホストシステム2は、自身が算出した暗号化情報と、ドライブ1から得られた暗号化情報とを比較して、一致していれば両者の暗号化手順が同一であり、第1段階の認証処理は成功であると判定する（ステップH9のYES）。一方、両者の暗号化情報が不一致の場合には、両者の暗号化手順が異なるため、認証処理は失敗となり、これ以後の手順は中止となる（ステップH9のNO）。

【0032】ホストシステム2での認証処理が成功すると、ディスクドライブ1での認証処理に移行する。以下図5のフローチャートを参照して、当該認証手順を説明する。

【0033】まず、ホストシステム2からの乱数発生要求に応じて、ドライブ1の認証モジュール20は、乱数発生回路201により乱数（疑似乱数）を生成する（ステップH10、D10）。ドライブ1は、生成した乱数をホストシステム1に送出する。

【0034】ホストシステム2は、ドライブ1から受信した乱数と、前の認証手順で算出した領域固有情報とを、暗号化機能部（暗号化プログラム）に与えて、暗号化情報（暗号化演算結果）を算出する（ステップH11）。ホストシステム2は、算出した暗号化情報をディスクドライブ1に送出する。一方、ディスクドライブ1では、認証モジュール20は、生成した乱数と領域固有情報101Bとを暗号化・復号化回路200に与えて、

9

暗号化演算を実行し、演算結果である暗号化情報を算出する（ステップD11）。

【0035】認証モジュール20は、自身が算出した暗号化情報と、ホストシステム2から得られた暗号化情報とを比較して、一致していれば認証処理が成功であると判定する（ステップH12のYES）。これにより、ディスクドライブ1は、ホストシステム2からの秘匿領域101に対するアクセス要求を許可し、当該秘匿領域101から読出した情報（復号化に必要な鍵情報）をホストシステム2に転送する。一方、両者の暗号化情報が不一致の場合には、認証モジュール20は認証処理が失敗として判定する（ステップH12のNO）。この場合には、ホストシステム2からの秘匿領域101に対するアクセス要求は、認められない。

【0036】以上のように同実施形態の認証手順により、ディスクドライブ1は、自身と同一方式の暗号化・復号化機能（暗号化・復号化プログラム）を備えているホストシステム2に対してのみ、秘匿領域に対するアクセスを許可する。この場合、秘匿領域に対する領域固有情報の交換をすることなく、両者が有する暗号化・復号化機能（暗号化・復号化プログラム）の方式が同一であるかを判定する。従って、秘匿領域に対応する領域固有情報が外部に漏洩することなく、高いセキュリティ性を確保できる。なお、秘匿領域に対するアクセス許可は、1回のみとする制限を設けることが望ましい。さらに、ディスクドライブ1は、秘匿領域から読出した情報をホストシステム2に送出する場合に、認証手順で送出した乱数で暗号化した情報を送出することが、セキュリティの面で望ましい。

【0037】また、ディスク10上の秘匿領域101～103は、通常使用領域である非秘匿領域100と比較して、認証処理を要するため、アクセス時間が増大する。そこで、秘匿領域101～103に格納する情報は、非秘匿領域100に格納（ダウンロード）したコンテンツデータ（暗号化データ）の復号化に必要な鍵情報などに制限することが望ましい。

【0038】（鍵情報と領域固有情報の更新処理）図7は、ディスク10上の秘匿領域101～103に格納されている鍵情報101A～103A、及び領域固有情報101B～103Bを更新するときの手順を示すフローチャートである。

【0039】まず、前述の認証手順により、ディスクドライブ1とホストシステム2間の認証処理を実行して、ホストシステム2は、ディスク10上の指定された秘匿領域101に対してアクセスが可能であるとする（ステップH20、D20）。ホストシステム2は、ディスクドライブ1が有する暗号化・復号化機能に関する情報（暗号化機能情報とする）を要求する（ステップH21）。この暗号化機能情報は、認証モジュール20が有する暗号化・復号化回路200での暗号化・復号化機

(6) 特開2002-229859

10

能の種類（方式）を示す情報であり、具体的には方式名又はプログラム名に相当する。

【0040】ディスクドライブ1は、認証モジュール20が有する暗号化・復号化機能の種類（方式）を示す暗号化機能情報をホストシステム2に送出する（ステップD21）。ホストシステム2は、受信した暗号化機能情報から、ドライブ1が有する暗号化・復号化機能の方式（復号種類）を認識する。ホストシステム2は、それらの中で新たに設定する方式に対応する暗号化手順（システムが有する暗号化プログラム）で、新たな鍵情報（更新情報）を構成する（ステップH22）。この新たな鍵情報は、ホストシステムが指定した秘匿領域101に対応する更新情報である。

【0041】さらに、前述の認証手順による再度の認証処理が実行された後に、ホストシステム2は、新しく構成した鍵情報及びその暗号化手順（暗号化プログラム）を示す情報（方式名）をディスクドライブ1に送出する（ステップH24）。ディスクドライブ1では、ホストシステム2から受信した鍵情報を仮情報として、ディスク10上の所定領域またはフラッシュメモリ16に格納する（ステップD23）。また、ホストシステムから指定された方式の暗号化手順（暗号化プログラム）を示す情報もディスク10上の所定領域またはフラッシュメモリ16に格納する。

【0042】ディスクドライブ1では、ホストシステムからの情報で指定された方式の暗号化手順で、ホストシステムから与えられた新しい鍵情報とドライブ1D情報とを使用して、秘匿領域101に対応する仮の領域固有情報を算出する（ステップD24）。具体的には、認証モジュール20の暗号化・復号化回路200は、ホストシステムからの情報で指定された方式の暗号化手順で、仮の領域固有情報を算出する暗号化演算を実行する。

【0043】次に、ホストシステム2とディスクドライブ1とは、前述の認証手順を実行する（ステップH25、D25）。但し、この認証手順で使用する鍵情報及び領域固有情報は、いずれも更新された仮の鍵情報及び仮の領域固有情報である。また、暗号化手順（方式）は、ホストシステム2から指定されたものである。この認証手順により、ディスクドライブ1からの暗号化情報と、ホストシステム2からの暗号化情報とが一致した場合には、認証処理は成功となる。従って、ホストシステム2とディスクドライブ1との間で、指定された秘匿領域101に対する鍵情報と領域固有情報の更新が確認されたことになる。

【0044】ホストシステム2は、ディスクドライブ1に対して、新たな鍵情報と領域固有情報の更新を要求する（ステップH26）。これにより、ディスクドライブ1は、仮の鍵情報及び仮の領域固有情報をそれぞれ更新情報として、正式に所定領域（秘匿領域101に確保されたエリア）に登録する（ステップD26）。また、認

(7)

特開2002-229859

11

証モジュール20は、ホストシステム2から指定された方式の暗号化手順(暗号化プログラム)を暗号化・復号化回路200に設定することになる。

【0045】以上のような更新機能により、初期時に設定されている秘匿領域101～103に対応する鍵情報101A～103A及び領域固有情報101B～103Bを、更新することができる。従って、ディスク10上の秘匿領域に対して、高度のセキュリティを確保することが可能となる。なお、秘匿領域をディスクドライブの製品出荷時の初期状態に戻す機能を用意しておくことが望ましい。この場合、鍵情報及び領域固有情報も初期状態に戻すことになるが、セキュリティの面から、秘匿領域に格納されている情報を、初期状態に戻すときに消去することが望ましい。

【0046】なお、同実施形態において、秘匿領域に対応する鍵情報101A～103A及び領域固有情報101B～103Bは、ディスク10上に格納されている場合を想定したが、これに限ることなく、フラッシュメモリ16に格納されている構成でもよい。また、認証モジュール20は、暗号化・復号化機能を実行する回路200を有し、当該回路200内で複数方式の暗号化・復号化手順を設定できる用に構成されている。しかし、内部のフラッシュメモリ202に複数方式の暗号化・復号化手順が格納されており、回路200は選択された暗号化・復号化手順で暗号化・復号化処理を実行する構成でもよい。また、同実施形態は、ハードウェアで構成された認証モジュール20を想定したが、CPU15がフラッシュメモリ16に格納されたプログラムにより、同実施形態の認証処理及び更新処理を実行する構成でもよい。

【0047】

【発明の効果】以上詳述したように本発明によれば、ディスク上に複数の秘匿領域を設定し、各秘匿領域毎に異なる認証機能を有するディスク記憶装置を提供することができる。このようなディスク記憶装置であれば、各秘匿領域ごとに、異なる暗号化・復号化方式に対応する鍵情報や、またはコンテンツの種類毎に異なる鍵情報を保存することが可能である。これにより、高度のセキュリティを確保できる暗号化・復号化方式を適用したシステ

12

ムを実現することが可能となる。また、各秘匿領域に対応する鍵情報及び領域固有情報を更新する更新機能を実現することにより、秘匿領域に対するセキュリティ性を向上することができる。

【0048】本発明の具体的適用分野としては、例えばパーソナルコンピュータやモバイル情報機器の交換型記憶装置として使用するためのカード型(又はモバイル型)ディスクドライブや、インターネットやLANなどに使用されるサーバ用ストレージ装置である。

10 【図面の簡単な説明】

【図1】本発明の実施形態に係るディスクドライブの要部を示すブロック図。

【図2】同実施形態に関するディスク上の記憶領域の構成を示す図。

【図3】同実施形態に関するフラッシュメモリの格納内容を示す図。

【図4】同実施形態に関する認証手順を説明するためのフローチャート。

20 【図5】同実施形態に関する認証手順を説明するためのフローチャート。

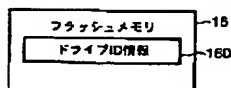
【図6】同実施形態に関する認証モジュールの内部構成を示すブロック図。

【図7】同実施形態に関する認証機能に含まれる情報更新手順を説明するためのフローチャート。

【符号の説明】

- 1…ディスクドライブ
- 2…ホストシステム
- 3…記録媒体(メモリカード)
- 4…インターネット
- 10…ディスク
- 11…スピンドルモータ
- 12…ヘッド
- 13…データチャネル
- 14…ディスクコントローラ
- 15…CPU
- 16…フラッシュメモリ
- 20…認証モジュール
- 101～103…秘匿領域

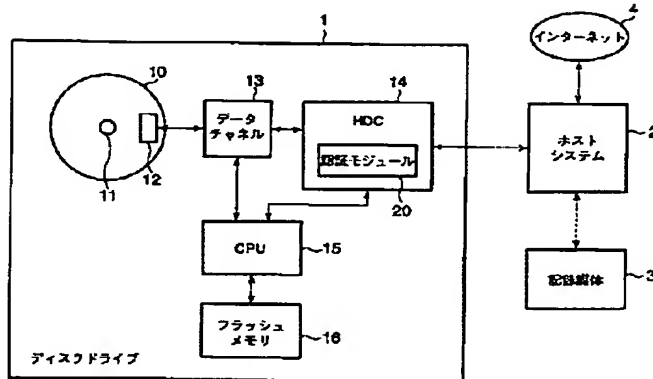
【図3】



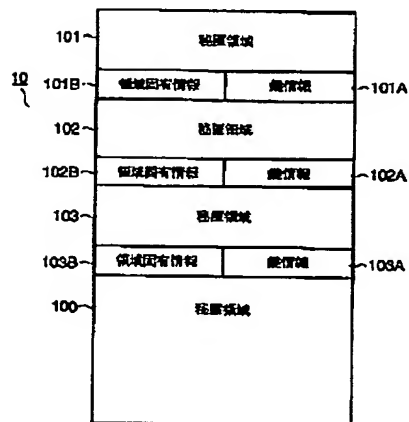
(8)

特開2002-229859

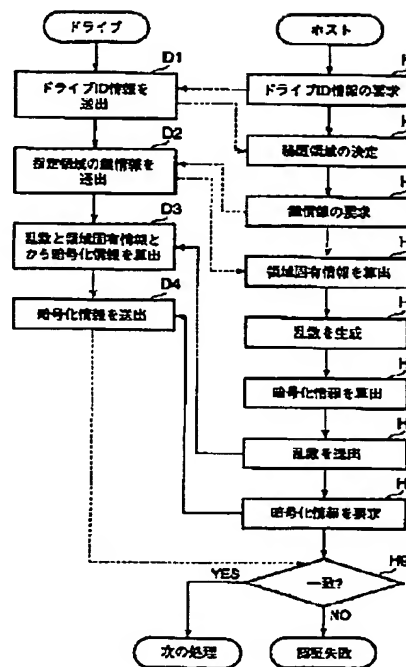
【図1】



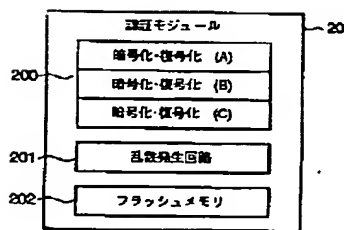
【図2】



【図4】



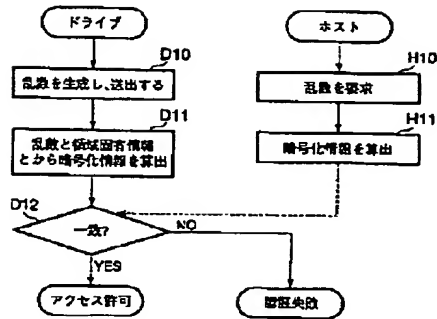
【図5】



(9)

特開2002-229859

【図5】



【図7】

